A. JOSEPH DeNUCCI
AUDITOR

The Commonwealth of Massachusetts

AUDITOR OF THE COMMONWEALTH
ONE ASHBURTON PLACE, ROOM 1819
BOSTON, MASSACHUSETTS 02108
TEL (617) 727-6200

2001-0031-4C

OFFICE OF THE STATE AUDITOR'S
REPORT ON EXAMINATION OF
INFORMATION TECHNOLOGY-RELATED CONTROLS AT
THE BUREAU OF SPECIAL INVESTIGATIONS

July 1, 1999 to July 11, 2001

OFFICIAL AUDIT REPORT
NOVEMBER 2, 2001

2001-0031-4C

TABLE OF CONTENTS

INTRODUCTION

The Bureau of Special Investigations was established in 1971 as the Bureau of Welfare Auditing by Chapter 22, Section 15B, of the Massachusetts General Laws. The Bureau had the authority to investigate fraud within any program administered by the Massachusetts Department of Public Welfare, now the Department of Transitional Assistance (DTA), and the Medicaid program, which is currently administered by the Division of Medical Assistance (DMA). The Bureau of Welfare Auditing was governed under the then newly-established Fraudulent Claims Commission. The name of the Bureau was changed to the Bureau of Special Investigations in July 1980 and the authority of the Bureau was expanded to include any program administered by the Department of Social Services (DSS). In 1992, the Bureau became part of the Department of Public Safety as part of a consolidation of law enforcement agencies. A legislative change in November 1999 moved the Bureau under the purview of the Department of Revenue (DOR).

The mission of the Bureau is to conduct investigations of alleged fraud in public assistance programs, deter fraud prior to the awarding of public assistance grants, and investigate individuals and organizations involved in fraudulent activities. The Bureau investigates complaints and initiates investigations of circumstances where there are indications of the possibility of a fraudulent claim for payment or services under any assistance program administered by the Department of Transitional Assistance, Department of Social Services (DSS), DMA, or receipt of payments by persons not entitled to benefits pursuant to Massachusetts General Laws, Chapter 14, Sections 9-11. The Bureau investigates individuals and organizations referred by DTA and other sources and refers cases for prosecution where sufficient evidence exists of a possible fraud. These individuals include recipients of public assistance, vendors, and public employees. In addition, the Bureau maintains a front-end detection program that screens and deters potentially fraudulent public assistance applications and a Warrant Unit to locate and apprehend persons wanted on arrest warrants as the result of an investigation. The Warrant Unit is also responsible for the coordination of arrests of recipients of public assistance wanted on warrants unrelated to public assistance fraud. In certain instances, Medicaid provider or vendor fraud is referred to the Medicaid Fraud Control Unit (MFCU) of the Massachusetts Attorney General's Office.

The Bureau uses information technology in support of its overall mission. The Bureau's information technology mission is to use stable, proven computer technologies in support of its case tracking function and to maintain an effective automation and communications system. Through the DOR computer network, the Bureau has access to DOR taxpayer information, as well as to DTA, DMA, Registry of Motor Vehicles (RMV), and other agency records pertaining to background information and investigations. The Bureau's central office monitors the progress of each case and reports monthly to the Bureau Director, who in turn provides a report to the Governor, the legislature, and other agencies.

The DOR's Information Services Organization (ISO) Division oversees the Bureau's IT-operations. The Bureau's operations are augmented by DOR's network, located in Chelsea, which provides network support. The Bureau's primary administrative application system is a state-developed system that was created in 1997 by the Information Services Organization of the Executive Office of Public Safety. The system, known as the Case Tracking System, is an integrated application, which operates at the Massachusetts Information Technology Center in Chelsea. The tracking system utilizes a Microsoft Access-based software package to manage and track fraud cases from their initial referral to the conclusion of the case investigation. The Bureau's other automated systems include Microsoft NT 4.0 and Novell Netware applications.

At the time of our audit, the primary administrative information technology (IT) services for BSI were supported by a file server used at the central office for individual file storage and file sharing and a DOR file server at the Chelsea data center. These servers had been custom built and configured to replace the servers transferred from the Department of Public Safety to DOR's Chelsea data center. The Bureau's network consists of a Microsoft NT file sever connecting thirty workstations. All thirty workstations have access to certain of the Commonwealth's administrative systems through Massachusetts Access to Government Network (MAGNET) Wide Area Network (WAN). The BSI also uses several software packages, including Windows 95 and Office 97 Professional.

As of June 30, 2001, the Bureau was comprised of a central office in Boston and 35 area offices located throughout the Commonwealth. The Bureau operated with an annual budget of approximately $5 million for fiscal year ended June 30, 2001, of which $2.8 million was reimbursed by various federal agencies. The Office of the State Auditor's examination focused on an evaluation of the Bureau's IT-related general controls and controls over and within the Case Tracking System.

AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY

Audit Scope

From February 9, 2001 to July 11, 2001, we performed an information technology (IT) audit at the Bureau of Special Investigations (BSI). Our audit scope included a review of IT-related general controls for the period July 1, 1999 through July 11, 2001. We reviewed IT-related controls pertaining to organization and management, physical security, environmental protection, business continuity planning, on-site and off-site backup media storage, system access security, hardware and software inventory, and use of authorized software. We also reviewed BSI's monitoring of cases through the Case Tracking System from case referral to case resolution. Additionally, we reviewed compliance with the monthly filing requirements contained in Massachusetts General Laws, Chapter 14, Section 11, paragraph 8.

Audit Objectives

The primary objective of our audit was to determine whether adequate controls were in place and in effect for selected IT and administrative control areas. We sought to determine whether the Bureau's IT-related internal control environment, including policies, procedures, practices, and organizational structure provided reasonable assurance that control objectives would be achieved to support business functions. We sought to determine whether the Bureau provided adequate organization and management for IT-related functions with respect to oversight, documentation of policies and procedures, and monitoring and evaluation of IT operations. We further sought to determine whether adequate physical security controls were in place to provide reasonable assurance that access to the computer room areas and the Bureau's central location at the administrative office was limited to only authorized personnel. With respect to environmental protection, our objective was to determine whether controls were adequate to prevent and detect damage to, or loss of, IT-related equipment and media for the computer room housing the mainframe computer at the Department of Revenue's Chelsea operations and for the areas housing the Bureau's file server and work stations at the administrative office.

We evaluated whether an effective business continuity and contingency plan had been developed and implemented to provide reasonable assurance that mission-critical and essential IT operations could be regained within an acceptable period of time should a disaster cause computerized operations to fail or become inaccessible. We also sought to determine whether adequate controls were in place to provide reasonable assurance that backup copies of all magnetic media were being generated on a regular basis and whether they were properly accounted for and labeled. In addition, we sought to determine whether the Bureau had made proper provisions to ensure that copies of backup media were stored on-site and off-site in a secure and environmentally protected and controlled location so that the system and data files could be restored should a disaster occur and business continuity plans need to be exercised.

We sought to determine whether adequate system access security controls were in place to provide reasonable assurance that only authorized users would have access to the BSI's automated systems. We further sought to determine whether adequate controls were in place to prevent and detect unauthorized access to data and systems and whether the senior IT staff were notified when users terminated employment or when there was a change in job functions that would require the user's access privileges to be changed or deactivated.

With respect to hardware and software inventory, we reviewed BSI's written policies and procedures regarding the proper accounting for and safeguarding of IT-fixed assets. We also evaluated whether computer hardware and software were safeguarded from unauthorized use and theft, whether these assets were adequately reflected in the fixed-asset inventory and accounting records, and whether an annual physical inventory was conducted. We also evaluated controls regarding the use of authorized software and whether copies of software licenses were on file for microcomputer and LAN-based software.

In conjunction with our review of the internal control environment, we determined whether the Bureau had developed and implemented written, authorized, and approved IT-related internal control policies and procedures for maintaining and monitoring cases processed through the Case Tracking System. Furthermore, we sought to determine whether the Bureau's Case Tracking System and monitoring procedures were sufficiently comprehensive to track information on the investigation, status and resolution of fraud cases and whether the Bureau was in compliance with its statutory requirements to file monthly activity reports with the Governor and the state legislature.

Audit Methodology

To determine the audit scope and objectives, we conducted pre-audit work, which included obtaining and recording an understanding of relevant operations and reviewing documentation regarding BSI's mission, operations, and IT organization and management. We interviewed DOR's Information Services Organization (ISO) Division's staff and the Bureau's senior administrative staff to gain an understanding the Bureau's operations and information technology control environment. In conjunction with our review of the internal control environment, we evaluated the Bureau's written, authorized, and approved IT-related internal control policies and procedures for maintaining and monitoring cases through the case tracking system.

To accomplish a preliminary review of the adequacy of general controls over IT-related functions and assets, we obtained an understanding of and observed computer operations at BSI's central office. We also conducted a site visit to one of BSI's area offices and DOR's Chelsea data center, and performed a risk analysis of computer operations and related areas. To assess the adequacy of IT general controls, we interviewed BSI staff and DOR's ISO Division staff, observed operations, and performed selected audit tests.

Regarding our review of IT organization and management, we interviewed senior management, reviewed and analyzed relevant documentation, and assessed selected organization and management controls. To determine whether IT-related assets, including LAN and microcomputer-based data files and software at the BSI's administrative office and BSI's IT operations at the DOR Chelsea data center, were adequately safeguarded from damage or loss, we reviewed physical security and environmental protection over computer operations through observation and interviews with BSI and ISO Division management and staff.

To assess the adequacy of disaster recovery and business continuity planning, we determined whether formal planning had been performed to resume computer operations in a timely manner should automated systems be damaged or destroyed or otherwise rendered inoperable. In addition, we interviewed ISO Division and BSI staff to determine whether a written, tested business continuity plan was in place, whether the criticality of application systems had been assessed, and whether risks and exposures to computer operations had been evaluated. We reviewed the internal control documentation regarding business continuity planning developed by the DOR's ISO Division management. Further, we evaluated the adequacy of provisions for on-site and off-site computer backup media through interviews and observations. We inspected the on-site media storage location, but did not visit the off-site location.

Our examination of system access security controls included a review of access privileges of those employees authorized to access the mainframe and microcomputer systems. To determine whether existing system-based access privileges were authorized and reflected current responsibilities, we reviewed procedures for granting and updating system access and preformed selected tests. To determine

whether access security was being properly maintained through the management of user-IDs and passwords, we interviewed the senior IT staff and assessed the level of access security being provided. We performed tests, such as comparing a systems generated user access list to a current official list of employees, to determine whether only authorized users had access to BSI's data files and programs. Further, we reviewed the access privileges of selected system users by determining whether those users were restricted to only the application programs and data files to which they had been authorized. We determined whether procedures were in place to ensure that the ISO Division was promptly and properly notified when a change in personnel status (e.g., employment termination, job transfer, or leave of absence) occurred so that the user-ID and password could be promptly deactivated from the system or the access privileges appropriately modified.

We conducted interviews and reviewed control documentation from BSI management to determine the adequacy of hardware and software inventory control policies and procedures. We obtained and reviewed an IT-related assets inventory record, which comprised 30 workstations located at BSI's central office. To determine whether the BSI's hardware inventory records were current, accurate, and valid, we compared all computer hardware inventory items appearing on the ISO Division's computer hardware inventory listing to the actual computer hardware on hand. We performed a test of the inventory record, tracing 50% of items from the list to floor and tracing the remaining 50% from the floor to the list. To determine whether inventory records were current, accurate, and valid, we performed a test of items listed on the inventory list and compared them to their physical locations. We evaluated the adequacy of inventory controls through tests and observations by assessing the integrity of the inventory record, determining whether computer hardware was properly tagged with BSI identification numbers and in good condition, and whether the Bureau conducted an annual physical inventory of fixed assets and reconciliation to the inventory record.

We sought to determine whether adequate controls were in place to provide reasonable assurance that microcomputer and mainframe-based software would be properly accounted for. We initially reviewed software inventory control practices and procedures, and determined whether a current, accurate, complete, and valid software inventory record had been developed by examining the adequacy of the inventory records and then comparing software licenses to the software inventory records. We reviewed the list of software residing on the hard drives of 22 microcomputer systems installed at the BSI's administration office in Boston. We compared the software installed on the microcomputer hard drives to the list of the software inventory provided by the BSI to determine whether only authorized software was residing on BSI's automated systems. To determine whether adequate internal controls were in place regarding BSI's case tracking system, we interviewed senior staff at the central office and obtained and reviewed relevant policies, procedures, and system documentation regarding BSI's case tracking system. We used a software product known as Audit Command Language (ACL) to analyze

data and select samples for review from the Bureau's case tracking system. At one selected area office, we used a judgmental sample of 8 cases, each with an estimated fraud of between $2,000 and $10,000 and with an active status that went beyond BSI's six-month and one-year target due dates. We reviewed the selected cases to ascertain date received by area office, nature of alleged fraud, dollar amount of alleged fraud, current status of case, length of time open and reason for cases to be open beyond the specific target dates, and determined whether the case tracking system records reflected what was in the case documents. Using agency-supplied flow charts and through discussions with BSI staff and investigators, we evaluated the monitoring procedures used by the central office to track and evaluate the timeliness of case processing.

To determine whether adequate internal controls were in place to ensure compliance with the monthly reporting requirement, we evaluated six monthly reports that had been submitted to the Governor and Legislature during the period from December 2000 to May 2001. For each report selected, we traced information provided in the reports to source documents, and checked each report for compliance with "Procedures for the Production of BSI monthly reports to the Governor and the Legislature" which are written procedures established by BSI that explain how the accumulated information from the case tracking system screens are generated, and we then evaluated the accuracy of the report.

Our review was conducted in accordance with Generally Accepted Government Auditing Standards (GAGAS) of the United States and industry auditing practices. The audit criteria used for our control examination were based on applicable legal requirements, Bureau policies and standards, and control objectives and management control practices outlined in the Information Systems Audit and Control Foundation's IT governance model "Control Objectives for Information and related Technology (CobiT)," published in July 2000.

AUDIT SUMMARY

Based on our examination, we determined that controls in place provided reasonable assurance that control objectives pertaining to IT-related organization and management, physical security, system access security, environmental protection, business continuity planning and on-site and off-site backup computer media would be met. With respect to the selected administrative control areas, our review indicated that BSI had in place a comprehensive Case Tracking System to manage its ongoing fraud investigation cases and was meeting its filing obligations in compliance with the statutory requirement to file monthly activity reports with the Governor and the legislature. However, our audit revealed that controls needed to be strengthened with regard to the timely resolution of fraud cases.

Our review of IT-related organization and management disclosed that adequate organizational controls were in place, including the level of oversight provided by DOR's Information Services Organization (ISO) for BSI's IT operations. Our review disclosed that the ISO Division's existing computer policy and procedures manual was modified to include BSI's IT operations and controls, including organization and management, physical security, environmental protection, system access security, business continuity planning, on-site and off-site backup computer media storage, hardware and software inventory control, and the operation and use of the Case Tracking System. We found that IT-related policies and procedures were well documented, appropriate and updated on a regular basis.

We found that internal controls in place provided reasonable assurance of adequate physical security and environmental protection of BSI microcomputers and file servers at the BSI's central office South Boston location and DOR's IT facility in Chelsea. With respect to physical security, all personnel entering the facility are checked by building security in order to help prevent unauthorized access to BSI's computer environment. BSI central office and DOR's file servers in Chelsea are located in securely locked areas. Our audit also revealed that there were adequate environmental protection controls in place and operating, including fire-suppression devices, heat and smoke detectors to protect IT-related assets, and separate uninterrupted power supplies (UPS) and backup generators at the central office and Chelsea data center locations.

We found that the Bureau had a formal business continuity strategy and plan through the ISO Division to help ensure resumption of mission-critical and essential processing within an acceptable time frame should processing be rendered inoperable or inaccessible. In addition, procedures were in effect for on-site and off-site storage of backup copies of magnetic media to further ensure system availability. Although we did not evaluate the location where backup computer media were stored, our audit revealed that the area used for storage of on-site backup media was adequate and the DOR indicated that backup media were being sent to off-site storage were adequate to provide continued operations, if created and stored properly. However, since the business continuity plan had not been recently tested, and DOR had

not preformed an agency-specific criticality assessment of BSI's primary application, the Case Tracking System, we recommend that DOR, in conjunction with the Bureau, perform criticality assessments of BSI's IT operations and test the plan to ensure its viability.

Regarding system access security, we found that system access controls provided reasonable assurance that only authorized users had access to the BSI's data files and programs residing on computer and application systems. We found that administrative controls over user-IDs and passwords provided reasonable assurance that access privileges would be deactivated or appropriately modified should BSI employees terminate employment or incur a change in job requirements. Also, through observations and interviews we determined that administrative password protection and changes to passwords were adequately controlled through BSI's IT network. We also determined that access privileges granted to individuals were appropriate given their job responsibilities and functions. During the course of our audit, nothing came to our attention to indicate that there were weaknesses in access security to the Case Tracking System.

With respect to hardware and software inventory control, we found that the ISO Division was responsible for the acquisition, installation, and disposal of these items for the Bureau. We noted that DOR had documented inventory control policies and procedures and a current listing of all of BSI's hardware and software products. Although the stated policies and procedures provided reasonable assurance that all IT-related assets were adequately listed, identified, and controlled, and our review of inventory items located in the central office indicated that all of the items were locatable and properly accounted for, we found that certain control procedures needed to be strengthened. In particular, we found that BSI and the ISO Division were not performing an annual physical inventory, and agency-specific tags were not on any hardware inventory items located in the central office. Although we noted that all items could be located, were in good condition, and were being utilized, we recommend that BSI, in conjunction with DOR, formalize procedures for tagging all BSI IT equipment and conduct an annual physical inventory to validate information on the inventory list. We found appropriate controls in place regarding the maintenance of the inventory record for software products and licenses and the use of only authorized software. Subsequent to the completion of our field-work, BSI in conjunction with DOR stated in their response to our draft report that "ISO purchased inventory software and hardware that allows for the bar coding of all IT related inventories. A plan to begin the inventory process is currently being discussed."

Our review of BSI's Case Tracking System disclosed that controls over receipt of case referral, initial processing, accounting, transferring to area offices, and investigations were in place and the data elements were adequate for tracking case information. We also determined that the Case Tracking System data was valid and accurate through the input, updating and output stages. However, we determined that the monitoring of case referral resolution needed to be strengthened. We found that case

referrals from all sources remained on active status without a fraud calculation after the investigation was completed, and pending closure cases were not being resolved on a timely basis prescribed through BSI's established time frames. The delays were in part, attributable to only informal discussions taking place between area offices and BSI's central office, as well as changes to case status being made by the central office while the case was in the jurisdiction of the area office supervisor. As a result of cases not being resolved, recovery of potential fraud-related funds may not be maximized.

Our review of BSI's compliance with State statutory filing requirements regarding case maintenance and case resolution disclosed that the Bureau's procedures provided reasonable assurance that compliance objectives were being met and the Bureau had been filing the necessary reports with the Governor's office and legislature on a timely basis.

AUDIT RESULTS

Management of Case Tracking System

The Bureau's Case Tracking System is an automated application system used to track and monitor cases and related information being investigated by the Bureau. The Case Tracking System provides information regarding the processing of case referrals from their origin, allows screening and assigning of case referrals to area offices, provides descriptions of alleged fraud and estimates of fraud calculations, and tracks case investigations including due dates, transaction dates, and log-on dates. We found that the Case Tracking System was sufficiently comprehensive to meet the Bureau's stated needs for tracking information on investigations being processed through BSI and that the Bureau had generally adequate documented policies and procedures for the use of this application system. However, our examination of BSI's resolution of cases processed through the system revealed that, partly as a result of BSI not having formal communication with its regional and area offices regarding case resolution, the Bureau was not adequately monitoring and facilitating case resolution on a timely basis. Delays in case resolution have contributed to a backlog in case resolution of 3,008 active cases and recovery of fraud-related monies initiated on 40% of the 7,441 total open cases on hand as of June 1, 2001.

The Bureau is mandated to perform investigations of several types of alleged fraud. By management directive, investigations are to be completed and resolved within six months or one year in accordance with the Bureau's established time frame for the specific alleged offense. The six-month or one-year time period established by the Bureau to complete investigations and resolve the fraud begins as of the date the case referral is transferred to the applicable area office. At the completion of an investigation, a fraud calculation amount is determined for active cases. Lastly, collection procedures for both active and pending-closure case referrals are initiated.

At one area office, we judgmentally selected eight active cases for review, each with an estimated potential fraud of between $2,000 and $10,000 that had been open beyond the six-month and one-year due date. We performed a test on these cases to determine why the cases had extended beyond the established due date, evaluate the reliability of data, and determine whether BSI was adequately monitoring the overdue cases to help ensure their timely resolution. Regarding the reliability of information in the cases reviewed, we found the data to be accurate, complete, valid, and verifiable to case source documents. We tested these cases to ascertain date received by area office, nature of alleged fraud, dollar amount of alleged fraud, current status of case, length of time open, and reason for cases having been open beyond the six-month one-year time frame.

In addition to data captured through the Case Tracking System, our review indicated that investigators prepare and submit a hand-written chronology of information that is submitted to the central office. However, this information was not reflected in the Case Tracking System. During our review at

the Quincy area office, we noted that the investigator's list of active cases being maintained by the investigators that had a pending-closure status did not include a due date. We also noted that there were case referrals that changed from "pending closure" status to "warrant status" and that these cases were not always being maintained at the originally designated area office. In addition, BSI's staff at the Quincy area office indicated that they were unable to print certain screens within the Case Tracking System, which contained essential case tracking information regarding case resolution and disposition. Because area offices did not always share the case-related information on a routine bases, timely resolution may have been negatively affected.

We ascertained that the central office submits two reports or memoranda to BSI's area office supervisors based on information taken from the Case Tracking System. The first report, entitled "backlog of active/no calculation case referrals," lists assigned active status case referrals that are more than six months or one year beyond the due date for case resolution. The second report, entitled "unresolved pending closure/no warrant case referrals," lists assigned pending closure status case referrals which are beyond the six month or one year due date without resolution. While the first report was disseminated to the applicable investigator, the area office could not provide any evidence that the second report was disseminated at the time of our visit and no specific time change had been established for distribution for these reports. As a result, area office investigators may not be properly informed of cases that are overdue. Furthermore, we found no evidence to indicate that prompt action was taken with respect to the case referrals listed on the second report, i.e., cases pending closure and beyond allotted time limits. We also determined that the area investigators and supervisors did not report to the central office the reasons that the active and pending-closure status case referrals were unresolved beyond the established due date. As a result of the inadequate case management procedures with respect to sharing and disseminating information, case resolution was being hampered. We found that case status between area offices and the central office were not being adequately communicated and monitored.

Recommendation:

We recommend that the Bureau establish written policies with respect to the two reports generated from the central office to the area offices concerning overdue cases, to include provisions to require that the reports be issued on a monthly basis. We also recommend, that the area office supervisors and investigators document responses to these reports in the Case Tracking System, and promptly acknowledge receipt of these reports to central office. The policies should also describe how area supervisors should respond to the reports. We recommend that BSI through DOR modify the Case Tracking System to allow area supervisors to enter into the Case Tracking System on a timely basis, actual reasons that an active or pending case referral status case remains unresolved beyond due date.

Auditee's Response:

- *We will establish a written policy for communication between the Central and Area Offices pertaining to overdue cases. The policy will include a provision that notices of overdue cases are to be issued on a monthly basis and specify how area managers should acknowledge receipt of and respond to the notices.*

- *We will request our Information Services Organization (ISO) to modify our Case Tracking System to allow Area Office supervisors and investigators to enter the reasons why active or pending cases remain open beyond the due dates.*

Please note that DOR has upgraded BSI's computer hardware and software. Consequently, BSI employees now have access to shared folders that post the latest information on case activity, investigator inventory and performance in meeting due dates, and updates to all BSI policies and procedures. Additionally, operational improvements, such as remote PC help, have led to ISO's ability to provide better assistance to BSI's field staff.

Auditor's Reply:

We commend BSI for improving communication between its central office, area offices, and area office supervisors. We feel the improvements made to the case tracking will improve BSI's operational efficiency through timely resolution of cases.